Statement of Chair Jane Harman Subcommittee on Intelligence, Information Sharing & Terrorism Risk Assessment

"Internet Terror Recruitment and Tradecraft: How Can We Address an Evolving Tool While Protecting Free Speech?" (as prepared for delivery)

Wednesday, May 26, 2010

Recent terror attacks and plots have taught us that the lonely, vulnerable or disaffected are just a few mouse clicks away from terrorist recruiters.

The anonymity of the Internet and the sheer speed of communications across it make it an easy tool for recruitment and for streamlining terror group training and operations.

According to the FBI, the Christmas day bomber Umar Farouk Abdulmutallab was recruited on the internet and trained in just six weeks. A Philadelphia woman – Colleen LaRose, who assumed the name Jihad Jane online – apparently used YouTube and other websites to post communications about staging attacks in the US, Europe and South Asia.

Fort Hood shooter Major Malik Hasan used e-mail to contact an American cleric in Yemen, Anwar al Awlaki, who just last weekend posted another Internet video calling for the death of more civilians modeled after Hasan's point blank assault of deploying service members in a medical unit at Fort Hood. Hasan killed 13 and wounded 31.

Hasan's family attended the Dar al Hijrah Islamic Center in Falls Church, Va., where Awlaki was preaching in 2001, around the same time two 9/11 hijackers worshipped at the mosque.

Najibullah Zazi, who was arrested last year when his plot to bomb the New York subway was uncovered, searched beauty salon and home improvement store websites on multiple occasions for chemicals to make a bomb. He also researched bomb making instructions from Internet sites.

Adam Gadahn, an American citizen from California, now serves as al Qaeda's English-language spokesman under the pseudonym Azzam al Amriki. He has produced propaganda videos that are circulated over the Internet which encourage Muslims to join the global extremist movement and take part in "slitting the throats of the infidel."

The dilemma is that the Internet is a forum for free speech and global commerce – but the underside of that is it can also be a forum for violence and global terror. How to respect individual freedom and access, and yet find those who abuse the Internet and stop them before they act is a huge and difficult challenge.

Let me be clear: Liberty and security are not a zero sum game. We don't get more of one and less of the other. We get more of both – or less. In fact, we must. Security without the liberties that our Constitution protects and Americans treasure is not consistent with our values.

Our Subcommittee has been wrestling with this problem for a while. This is our third hearing on the threat posed to the U.S. homeland by violent extremism.

The purpose of today's hearing is to analyze the use of the Internet as a facilitator for recruitment training and development of terror plots. The problem is the Internet combines speed and anonymity in a way that complicates law enforcement and intelligence work exponentially.

I'm glad that Anthony Romero, the able executive director of the ACLU and well-known commentator on this issue, is here at my personal invitation to testify about how to guard the privacy and civil liberties of individuals who use the Internet for the right reasons. I consult Anthony regularly, and I thank him for his time.

In fact, the witnesses before us today, all close friends and colleagues have been enormously helpful to the Subcommittee as we evaluate strategies to prevent and disrupt terror threats. They have all thought deeply and written extensively on these topics,

Dr. Bruce Hoffman, a professor at Georgetown University, will discuss the evolving nature of terror network tactics on the Internet.

Brian Jenkins, a senior adviser at the RAND Corporation, will discuss his latest report, "Incidents of Jihadist Terrorist Radicalization in the US since 9/11."

Phil Mudd, who retired from the FBI this year as associate executive director of the National Security Branch, will discuss US efforts to conduct surveillance of internet communications and how the FBI currently intervenes.

We will also hear from John Morris, General Counsel for the Center for Democracy and Technology. Welcome to you all.

As difficult and controversial as this subject is, we need to find the right way and place to intercept those who would do us harm. Developing a strategy around the Internet is not optional. It has to be part of that equation.

###